CONTROL EQUIPMENT, MAINTENANCE DEVICE, INFORMATION PROCESSOR, AND MAINTENANCE SERVICE PROVIDING METHOD

Patent number: JP2004126754

Publication date: 2004-04-22

Inventor: NARISAWA FUMIO; MOTOYAMA ATSUHISA; YAMASHITA KENICHI

Applicant: HITACHI LTD

Classification:

- international: ***G05B23/02; H04L9/08; H04L9/32; H04Q9/00;*** **G05B23/02; H04L9/08; H04L9/32; H04Q9/00;** (IPC1-7): H04L9/08; H04L9/32; G05B23/02; G06F17/60; H04Q9/00

- european:

Application number: JP20020286969 20020930

Priority number(s): JP20020286969 20020930

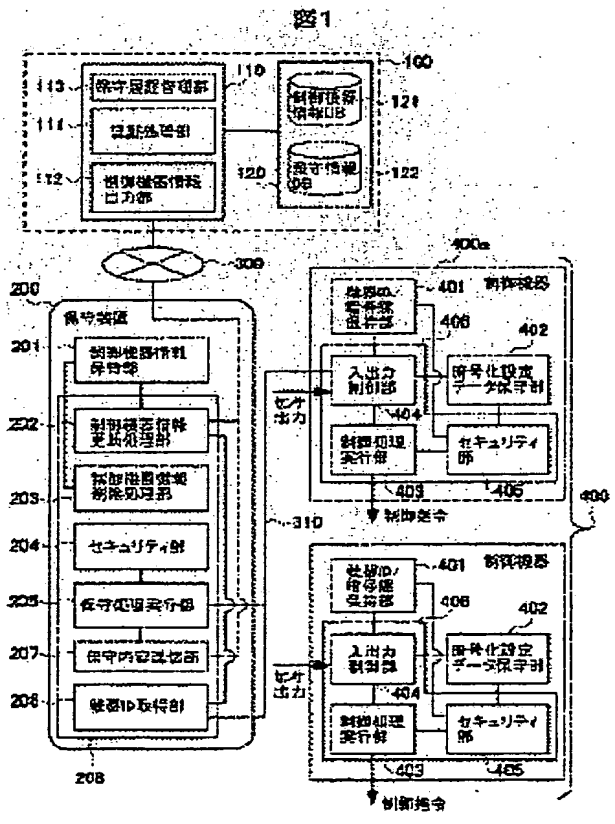
Report a data error here

Abstract of **JP2004126754**

PROBLEM TO BE SOLVED: To improve the security of technology information associated with equipment to be maintained.

SOLUTION: Control equipment 400a for controlling manipulated variables belonging to an object to be controlled is provided with an encryption setting data storing part 402 for storing the first encryption information of the target value of the manipulated variables, an equipment ID/encryption key storing part 401 for storing an encryption key to be used for decoding the encryption information of the equipment ID/encryption key storing part 401, and an arithmetic processing means 406 for outputting an instruction to be issued to the object to be controlled for making the manipulated variables close to the target value obtained by the decoding.

COPYRIGHT: (C)2004,JPO



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-126754
(P2004-126754A)
(43)公開日　平成16年4月22日(2004.4.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G05B 23/02	G05B 23/02	V	5H223
G06F 17/60	G06F 17/60	138	5J104
H04Q 9/00	G06F 17/60	512	5K048
// H04L 9/08	H04Q 9/00	301C	
H04L 9/32	H04Q 9/00	311J	

審査請求 未請求　請求項の数 19　OL　（全 18 頁）　最終頁に続く

(21)出願番号　特願2002-286969(P2002-286969)
(22)出願日　平成14年9月30日(2002.9.30)

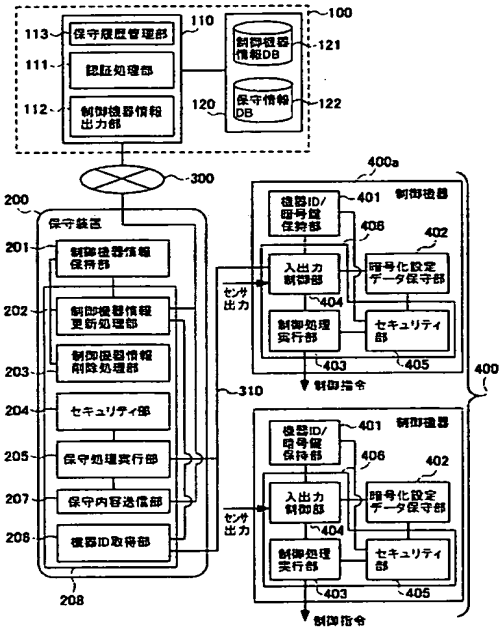
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100084032
弁理士　三品　岩男
(72)発明者　成沢　文雄
茨城県日立市大みか町七丁目１番１号　株式会社日立製作所日立研究所内
(72)発明者　本山　敦久
茨城県日立市大みか町七丁目１番１号　株式会社日立製作所日立研究所内
(72)発明者　山下　健一
茨城県ひたちなか市市毛１０７０番地　株式会社日立製作所ビルシステムグループ内

Ｆターム(参考)　5H223 AA05 AA09 CC08 DD03 EE06
最終頁に続く

(54)【発明の名称】制御機器、保守装置、情報処理装置および保守サービス提供方法

(57)【要約】
【課題】保守対象機器に関する技術情報のセキュリティ向上を図る。
【解決手段】制御対象に属する制御量を制御する制御機器４００ａに、前記制御量の目標値の第一暗号化情報が格納された暗号化設定データ保持部４０２、機器ＩＤ／暗号鍵記憶部４０１の暗号化情報の復号に用いられる暗号鍵が格納された機器ＩＤ／暗号鍵記憶部４０１、暗号化設定データ保持部４０２の暗号化情報を機器ＩＤ／暗号鍵記憶部４０１の暗号鍵で復号し、当該復号により得られた目標値に前記制御量を近づけるための、制御対象に与える指令を出力する演算処理手段４０６を設けた。
【選択図】　図１

図1



【特許請求の範囲】
【請求項１】
制御対象に属する制御量を制御する制御機器であって、
前記制御量に関わるデータの第一暗号化情報が格納された第一記憶手段と、
前記第一暗号化情報の復号に用いられる暗号鍵が格納された第二記憶手段と、
前記一記憶手段の第一暗号化情報を前記第二記憶手段の暗号鍵で復号し、当該復号により得られたデータに前記制御量を近づけるための、前記制御対象に与える指令を出力する演算処理手段と、
を有することを特徴とする制御装置。
【請求項２】
請求項１記載の制御装置であって、
保守装置に接続される保守装置用接続部を有し、
前記演算処理手段は、
前記制御量に関わるデータとして設定されるべきデータの第二暗号化情報を前記保守装置用接続部が受け付けると、当該第二暗号化情報で前記第一記憶手段の前記第一暗号化情報を更新する、
ことを特徴とする制御装置。
【請求項３】
請求項２記載の制御装置であって、
前記第二記憶手段または前記第一記憶手段には、当該制御装置に割り当てられた機器識別情報が格納され、
前記演算処理手段は、
前記保守装置からの要求に応じて、前記第二記憶手段または前記第一記憶手段から前記機器識別情報を読み出し、当該機器識別情報を前記保守装置用接続部から出力させる、
ことを特徴とする制御装置。
【請求項４】
請求項３記載の制御機器の保守装置用接続部に接続される制御機器用接続部と、
前記制御量に関わるデータとして設定されるべきデータの入力を受け付ける入力受付け手段と、
前記制御機器用接続部が前記機器識別情報を受け付けると、当該機器識別情報を用いて、前記制御装置用の暗号鍵を含む制御機器情報をホストからダウンロードする制御手段と、
を有し、
前記制御手段は、
前記入力受付け手段が前記データの入力を受け付けた場合に、前記制御機器情報用の暗号鍵を用いた暗号化により得られた、前記データの暗号化情報を前記第二暗号化情報として前記制御機器用接続部から出力する、
ことを特徴とする保守装置。
【請求項５】
請求項４記載の保守装置であって、
前記制御機器情報には、前記制御装置用の暗号鍵を用いた暗号化を前記制御手段に実行させるための保守プログラムが含まれることを特徴とする保守装置。
【請求項６】
請求項４記載の保守装置であって、
前記制御手段が、前記制御機器情報を格納する制御機器情報記憶手段を備え、
前記制御装置の保守点検作業が終了した場合に、または、予め定めたタイミングで、前記制御手段は、当該制御装置の前記制御機器情報を前記制御機器情報記憶手段から削除することを特徴とする保守装置。
【請求項７】
請求項５記載の保守装置であって、
前記制御手段が、前記制御機器情報を格納する制御機器情報記憶手段を備え、

前記制御装置の保守点検作業が終了した場合に、または、予め定めたタイミングで、前記制御手段は、当該制御装置の前記制御機器情報を前記制御機器情報記憶手段から削除することを特徴とする保守装置。

【請求項８】

請求項４記載の保守装置と通信する情報処理装置であって、

前記制御機器の制御機器情報を当該制御機器の機器識別情報に対応付けて記憶した記憶手段と、

前記保守装置から前記制御装置の機器識別情報を受け付けると、当該機器識別情報に対応付けられた制御機器情報を前記記憶手段から読み出し、当該制御機器情報を、前記保守装置に送信すべく出力する制御機器情報出力手段と、

を有することを特徴とする情報処理装置。

【請求項９】

請求項５記載の保守装置と通信する情報処理装置であって、

前記制御機器の制御機器情報を当該制御機器の機器識別情報に対応付けて記憶した記憶手段と、

前記保守装置から前記制御装置の機器識別情報を受け付けると、当該機器識別情報に対応付けられた制御機器情報を前記記憶手段から読み出し、当該制御機器情報を、前記保守装置に送信すべく出力する制御機器情報出力手段と、

を有することを特徴とする情報処理装置。

【請求項１０】

請求項６記載の保守装置と通信する情報処理装置であって、

前記制御機器の制御機器情報を当該制御機器の機器識別情報に対応付けて記憶した記憶手段と、

前記保守装置から前記制御装置の機器識別情報を受け付けると、当該機器識別情報に対応付けられた制御機器情報を前記記憶手段から読み出し、当該制御機器情報を、前記保守装置に送信すべく出力する制御機器情報出力手段と、

を有することを特徴とする情報処理装置。

【請求項１１】

請求項８記載の保守装置と通信する情報処理装置であって、

前記制御機器の制御機器情報を当該制御機器の機器識別情報に対応付けて記憶した記憶手段と、

前記保守装置から前記制御装置の機器識別情報を受け付けると、当該機器識別情報に対応付けられた制御機器情報を前記記憶手段から読み出し、当該制御機器情報を、前記保守装置に送信すべく出力する制御機器情報出力手段と、

を有することを特徴とする情報処理装置。

【請求項１２】

請求項９記載の情報処理装置であって、

制御機器に対する保守点検作業が実行される日付を表す日付情報を当該制御機器の機器識別情報に対応付けるスケジュール情報が格納された保守スケジュール記憶手段を有し、

前記スケジュール情報が、前記保守装置からの機器識別情報と当該機器識別情報を受け付けた日付を表す日付情報とを対応付けている場合に、前記制御機器情報出力手段は、前記制御機器情報記憶手段から読み出した制御機器情報を出力することを特徴とする情報処理装置。

【請求項１３】

請求項８記載の情報処理装置と、

請求項４記載の保守装置と、

を備えることを特徴とする保守システム。

【請求項１４】

請求項９記載の情報処理装置と、

請求項５記載の保守装置と、

を備えることを特徴とする保守システム。
【請求項１５】
制御対象に属する制御量を制御する制御装置の保守点検に用いる保守装置をホストで管理する保守サービス提供方法であって、
前記制御装置は、
前記制御量に関わるデータの暗号化情報を復号し、当該復号により得られたデータに前記制御量を近づけるための、前記制御対象に与える指令を出力する演算処理手段を備え、
前記ホストは、
前記制御装置用の暗号鍵を含む制御機器情報を記憶した記憶手段と、
前記制御装置の制御機器情報を前記保守装置に送信する制御機器情報出力手段と、
を有し、
前記保守装置は、
前記制御量に関わるデータの入力を受け付ける入力受付け手段と、
前記入力受付け手段が受け付けた前記データを、前記ホストからダウンロードした制御機器情報に含まれる暗号鍵で暗号化し、当該暗号化により得られた情報を、前記暗号化情報として前記制御装置に出力する制御手段と、
を有し
当該サービス提供方法は、
前記ホストにおいて、前記制御機器情報出力手段が、前記保守装置からの要求に応じて、前記制御装置用の制御機器情報を前記保守装置に送信する処理を有することを特徴とするサービス提供方法。
【請求項１６】
制御対象に属する制御量を制御する制御装置の保守点検に、入力受付け手段および制御手段を有する保守装置を使用する保守サービス提供方法であって、
前記制御装置は、
前記制御量に関わるデータの暗号化情報が格納された暗号化情報記憶手段と、
前記保守装置から入力された暗号化情報で前記暗号化情報記憶手段の暗号化情報を更新し、前記暗号化情報記憶手段の暗号化情報の復号により得られたデータに前記制御量を近づけるための、前記制御対象に与える指令を出力する演算処理手段と、
を有し、
当該保守サービス提供方法は、
前記保守装置において、前記入力受付手段が、ユーザから、前記制御量に下Ｋ割るデータとして設定されるべきデータの入力を受け付けると、前記制御手段が、当該データの暗号化情報を前記制御装置に出力する処理を含むことを特徴とする保守サービス提供方法。
【請求項１７】
請求項１６記載のサービス提供方法であって、
前記保守装置において、前記入力受付手段が受け付けたデータを暗号化するための、前記制御装置用の暗号鍵を含む制御機器情報を、前記制御手段が、ホストからダウンロードする処理を含むことを特徴とするサービス提供方法。
【請求項１８】
請求項１５記載のサービス提供方法であって、
前記制御機器情報には、前記制御装置用の暗号鍵を用いた暗号化を前記保守装置の制御手段に実行させるための保守プログラムが含まれることを特徴とするサービス提供方法。
【請求項１９】
請求項１６記載のサービス提供方法であって、
前記制御機器情報には、前記制御装置用の暗号鍵を用いた暗号化を前記保守装置の制御手段に実行させるための保守プログラムが含まれることを特徴とするサービス提供方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、制御機器の保守点検業務に係り、保守対象機器に関する技術情報の漏洩を防止するための技術に関する。

【０００２】

【従来の技術】

電話回線を利用して、保守会社の受信装置との間で情報通信を行うことができるエレベータ監視用端末装置が知られている（特許文献１参照）。このエレベータ監視用端末は、エレベータ機械室に設置され、エレベータ制御装置と伝送ラインで接続されている。そして、このエレベータ監視用端末は、個別仕様更新データを含むデータ変更指令を外部（保守会社）から受け付けると、その正当性を検証し、その結果、正当性が確認されたときのみ、ＥＥＰＲＯＭ内の個別仕様データを個別仕様更新データで上書きする。個別使用データの例としては、エレベータ監視端末の登録番号、エレベータの各種仕様情報、保守会社の受信装置に発報するとき用いる電話番号、エレベータの使用状況を保守会社に通知する時刻データ（定時発報時刻データ）が挙げられている。

【特許文献１】

特開平５－２７０７６２号公報

【０００３】

【発明が解決しようとする課題】

ところが、監視と異なり、保守点検作業は、保守員が、機器の設定データと実際の機器の動作とを比較しながら行う必要がある。このとき保守員が扱う設定データ等の、保守対象機器に関する技術情報は、保守管理者にとって機密にすべき重要な情報である。

【０００４】

そこで、本発明は、保守対象機器に関する技術情報のセキュリティ向上を目的とする。

【０００５】

【課題を解決するための手段】

本発明の一態様において、

制御対象に属する制御量を制御する制御機器に、

前記制御量に関わるデータの第一暗号化情報が格納された第一記憶手段と、

前記第一暗号化情報の復号に用いられる暗号鍵が格納された第二記憶手段と、

前記一記憶手段の第一暗号化情報を前記第二記憶手段の暗号鍵で復号し、当該復号により得られたデータに前記制御量を近づけるための、前記制御対象に与える指令を出力する演算処理手段とを設けた。

【０００６】

【発明の実施の形態】

以下、添付図面を参照しながら、本発明に係る実施の一形態について説明する。

【０００７】

まず、本実施の形態に係る制御機器保守システムおよびその保守対象となる制御機器の概略構成について説明する。

【０００８】

図１に示すように、本実施の形態に係る制御機器保守システムは、点在する複数の制御機器４００のなかの任意の機器に接続可能な携帯情報端末（保守装置）２００、制御機器の制御機器情報をネットワーク３００経由で保守装置２００に提供する管理システム１００を有している。なお、ここでは、保守装置２００が、制御機器群４００のなかの制御機器４００ａにケーブル３１０で接続された構成例を示してある。

【０００９】

保守装置２００は、ワイヤレスモデム等の無線通信装置やイーサネット（登録商標）等の有線通信装置が装着される接続口、接続中の制御機器の保守のために準備された制御機器情報（保守処理が定義された保守プログラム、制御対象に属する制御量に関わるデータ（本実施の形態では目標値）として設定されているデータのアドレスを含む機器情報、暗号鍵）がネットワーク３００を介してインストールされるとともに各種プログラム（ＯＳ、ダウンロードプログラム、復号処理が記述された復号プログラム等）が予めインストール

されたフラッシュメモリ、ＲＡＭ、タブレット付き液晶ディスプレイ、ユーザからの入力（制御対象に属する制御量の目標値として設定されるべきデータ等）を受け付ける各種キー、フラッシュメモリからＲＡＭにロードしたソフトウエアを実行するＣＰＵ、外部機器（制御機器）に接続されるインタフェース等を有している。このようなハードウエア構成およびソフトウエアによって、この保守装置２００は、制御機器情報が格納される制御機器情報保持部２０１、制御機器の保守に関する処理を実行する制御部２０８を実現する。そして、制御部２０８には、（１）接続中の制御機器４００αから機器ＩＤをダウンロードする機器ＩＤ取得部２０６、（２）機器ＩＤ取得部２０６が取得した機器ＩＤに対応付けられた制御機器情報を保守管理ホスト１１０からダウンロードし、それら制御機器情報を制御機器情報保持部２０１に格納する制御機器情報更新処理部２０２、（３）接続中の制御機器４００αから暗号化データを受け付け、それを、制御機器情報保持部２０１中の暗号鍵で復号するセキュリティ部２０４、（４）接続中の制御機器４００αの保守処理を実行する保守処理実行部２０５、（５）接続中の制御機器４００αの保守点検作業が終了したら、保守員による保守点検作業の履歴を管理システム１００に送信する保守内容送信部２０７、（６）接続中の制御機器４００αの保守点検作業が終了したら、制御機器情報保持部２０１から制御機器情報を削除する制御機器情報削除処理部２０８、が含まれる。保守員は、これらの機能構成を利用することによって、保守装置２００に接続中の制御機器４００αの保守点検作業（動作確認、動作変更、不具合の修正等）を行うとともに、自身の保守点検作業履歴を管理システムに報告することができる。

【００１０】

また、管理システム１００には、ネットワーク３００に接続された情報処理装置（保守管理ホスト）１１０、２種類のデータベース（制御機器情報データベース１２１、保守情報データベース１２２）および保守対象となる制御機器群４００の各機器ごとに準備された保守プログラムおよび機器情報が格納された外部記憶装置１２０、が含まれている。

【００１１】

制御機器情報データベース１２１には、図２に示すように、保守対象となる制御機器ごとに、その制御機器に割り当てられた機器ＩＤ１２１Ａ、その制御機器が保持する暗号鍵と同じ暗号鍵１２１Ｃ、その制御機器の保守点検のために準備された保守プログラムおよび機器情報の格納領域のアドレス情報１２１Ｂ、があらかじめ登録されている。

【００１２】

また、保守情報データベース１２２には、図３に示すように、制御機器の保守点検作業が終了するごとに保守情報が格納される。保守情報には、制御機器の機器ＩＤ１２２Ａ、保守点検作業が行われた日付１２２Ｂ、保守員が行った保守点検作業の内容を表す情報１２２Ｃが含まれる。

【００１３】

そして、保守管理ホスト１１０は、ネットワークインタフェース、可搬型記憶媒体（ＣＤ－ＲＯＭ等）が装着されるドライブ、各種プログラム（ＯＳ、保守装置からのリクエストに応じて保守管理処理を実行するサーバプログラム等）がインストールされたハードディスク、ＲＯＭ、ＲＡＭ、管理者からのデータ入力を受け付ける入力装置（キーボード等）、ハードディスクまたはＲＯＭからＲＡＭにロードしたソフトウエアを実行するＣＰＵ等を有している。ハードディスクには、各種プログラムの他、保守員認証の際に参照されるパスワードファイル、機器認証の際に参照される保守スケジュールファイル、が格納されている。パスワードファイルには、図４に示すように、保守員ごとに認証情報（ユーザＩＤ１１４Ａ、パスワード１１４Ｂ）１１４が記述されている。保守スケジュールファイルには、図５に示すように、各保守員ごとに、その保守員のユーザＩＤ１１５Ａ、その保守員が保守点検作業を行う制御機器の機器ＩＤと保守点検日付との対応情報のリスト（スケジュール情報）１１５Ｂが記述されている。

【００１４】

このようなハードウエア構成およびソフトウエアによって、この保守管理ホスト１１０は、（１）外部からアクセスがあった場合に認証処理を実行する認証処理部１１１、（２）

正当な保守員からのリクエストに応じて、制御機器情報データベース１２１に対するデータベース処理を実行し、これにより得られた制御機器情報を出力する制御機器情報出力部１１２、（３）正当な保守員からのリクエストに応じて、保守情報データベース１２２に対するデータベース処理を実行する保守履歴管理部１１３、を実現する。このような機能構成により、この保守管理ホスト１１０は、正当な保守員からのアクセスに対してのみ、その者が保守点検を担当する制御機器の制御機器情報を返信し、その者による保守点検作業の履歴を保存する。

【００１５】

一方、このような制御機器保守システムの保守対象となる制御機器群４００に含まれる各制御機器は、それぞれ、制御対象（モータ等）に関する制御処理を実行するマイクロコンピュータを有している。各マイクロコンピュータは、それぞれ、それを搭載する制御機器に割り当てられた機器ＩＤおよび制御対象の制御に必要な情報（制御対象の制御処理および保守装置との通信処理が定義された制御プログラム、復号プログラム、復号プログラムが用いる暗号鍵）が格納されたＲＯＭ、ＲＯＭから読み出した制御プログラムを実行するＣＰＵ、制御対象に属する制御量の目標値の暗号化データが格納されるＲＡＭ、外部装置（保守装置、各種センサ、制御対象）が接続されるインタフェース、ＣＰＵとインタフェース等との間のデータ転送を制御するシステムコントローラ等を有している。このようなハードウエア構成およびソフトウエアによって、各マイクロコンピュータは、（１）機器ＩＤおよび暗号鍵を保持する機器ＩＤ／暗号鍵保持部４０１、（２）暗号化データを保持する暗号化設定データ保持部４０２、（３）制御対象の制御処理および保守装置との通信処理を実行する演算処理部４０６、を実現する。そして、演算処理部４０６には、（４）保守装置等との間のデータ伝送を制御する入出力制御部４０４、（５）暗号化設定データ保持部４０２および機器ＩＤ／暗号鍵保持部４０１から暗号化データおよび暗号鍵を読み出し、その暗号化データをその暗号鍵で復号するセキュリティ部４０５、（６）セキュリティ部４０５の復号により得られた目標値にセンサ出力が近づくように、制御対象に属する制御量を制御する制御処理実行部４０３、が含まれている。

【００１６】

つぎに、図６により、本実施の形態に係る制御機器保守システムで実行される保守管理処理およびその保守対象となる制御機器が実行する処理について説明する。

【００１７】

保守員が、保守装置２００のインタフェースと、保守対象とする制御機器４００αのインタフェースとの間をシリアルケーブル３１０で接続してから、ダウンロードプログラムを起動すると（Ｓ５００）、保守装置２００の機器ＩＤ取得部２０６および制御機器情報更新処理部２０２が、以下の処理を実行する。

【００１８】

まず、保守装置２００の機器ＩＤ取得部２０６が、制御機器４００αに接続されたインタフェースから機器ＩＤの送信要求を出力する。この要求を受け付けた制御機器４００αでは、入出力制御部４０４が、機器ＩＤ／暗号鍵保持部４０１から機器ＩＤを読み出し、その機器ＩＤを、保守装置２００に接続されたインタフェースから出力する（Ｓ５０１）。これにより、保守装置２００の機器ＩＤ取得部２０６は、接続中の電気機器４００αの機器ＩＤを取得することができる。

【００１９】

その後、保守装置２００の制御機器情報更新処理部２０２は、保守管理ホスト１１０へアクセス要求を送信する（Ｓ５０２）。保守管理ホスト１１０の認証処理部１１１が、このアクセス要求に対して、認証の問いかけを返信すると、保守装置２００の制御機器情報更新処理部２０２が、図７に示すユーザ認証画面をディスプレイに表示させる（Ｓ５００）。このユーザ認証画面には、認証情報（ユーザＩＤ、パスワード）の入力を受け付ける入力ボックス６００，６０１、入力ボックス６００，６０１内のデータの消去指示を受け付けるキャンセルボタン６０３、入力ボックス６００，６０１内のデータの送信指示を受け付けるＯＫボタン６０２、が配置されている。保守員が、このユーザ認証画面上で、自己

の認証情報（ユーザＩＤ、パスワード）を入力ボックス６００．６０１に入力してからＯＫボタン６０２にタッチすると（Ｓ５０３）、制御機器情報更新処理部２０２は、その認証情報を含むユーザ認証要求を保守管理ホスト１１０に送信する（Ｓ５０４）。

【００２０】

保守管理ホスト１１０の認証処理部１１１は、ユーザ認証要求を受け付けると、それに含まれていた認証情報を用いて保守員認証処理を実行する。具体的には、保守管理ホスト１１０の認証処理部１１１は、認証情報に含まれていたユーザＩＤに対応するパスワードをパスワードファイルから取り出し、そのパスワードと、認証情報に含まれていたパスワードとを比較する。

【００２１】

その結果、両者が不一致であれば、保守管理ホスト１１０の認証処理部１１１は、ユーザ認証拒否を保守装置２００に返信する。

【００２２】

その反対に、両者が一致すれば、保守管理ホスト１１０の認証処理部１１１は、ユーザ認証確認を保守装置２００に返信する。これにより、以後、保守装置２００と保守管理ホスト１１０との間でデータ通信が可能となる。このようにして保守管理ホスト１１０と保守装置２００との間でデータ通信が可能となったら、保守装置２００の制御機器情報更新処理部２０２は、さらに、機器ＩＤを含む認証要求を保守管理ホスト１１０に送信する（Ｓ５０５）。

【００２３】

この機器認証要求に応じて、保守管理ホスト１１０の認証処理部１１１は、その要求に含まれていた機器ＩＤに対応する保守スケジュール情報を保守スケジュールファイルから取り出し、この保守スケジュール情報に、ログイン中の保守員のユーザＩＤと現在の日付との対応情報が含まれているか否かを検証する。

【００２４】

その結果、該当する対応情報が保守員リストに含まれていなければ、保守管理ホスト１１０の認証処理部１１１は、保守装置２００とのコネクションを切断する。

【００２５】

一方、該当する対応情報が保守員リストに含まれていれば、保守管理ホスト１１０の制御機器情報出力部１１２が、認証要求に含まれていた機器ＩＤを検索キーとして制御機器情報管理データベースを検索する。その結果、検索条件に合致するアドレス情報および暗号鍵が存在していれば、その暗号鍵およびそのアドレス情報が示す領域に格納された情報（保守プログラムおよび機器情報）を、制御機器４００αの制御機器情報として返信する（Ｓ５０６）。

【００２６】

制御機器情報更新処理部２０２は、保守管理ホスト１１０からの返信データを受け付けると、そのデータを制御機器情報保持部２０１に格納してから、制御機器情報のダウンロードが終了した旨のメッセージをディスプレイに表示させる。保守員は、このメッセージを参照することによって、制御機器４００αの保守点検作業を開始可能な状態、すなわち、図１５に示すように、保守装置２００に接続中の制御機器４００α用の制御機器情報（保守プログラム、機器情報、暗号鍵）が保守装置２００に格納された状態になったことを知ることができる。

【００２７】

そこで、制御機器情報のなかの保守プログラムを起動し（Ｓ５０８）、あらかじめ準備された保守コマンドのなかから選択したコマンドを保守装置２００に入力する。例えば、目標値として設定されているデータを参照する必要がある場合には、保守員は、制御量名を含む設定データ取得コマンドを保守装置２００に入力することができる。また、制御量の目標値として現在設定されているデータを参照する必要がある場合には、保守員は、制御量名を含む設定データ取得コマンドを保守装置２００に入力することができる。

【００２８】

保守装置の保守処理実行部２０５は、保守員からのコマンド入力を受け付けると、そのコマンドのコマンド名等を保守点検作業履歴として制御機器情報保持部２０１に格納する。さらに、保守員からのコマンドをセキュリティ部２０４に暗号化させ、それにより得られた暗号化データを含む処理実行リクエストを、制御機器４００αに接続されたインタフェースから出力する。このリクエストを受け付けた制御機器４００αでは、入出力制御部４０４が、
そのリクエストに含まれている暗号化データをセキュリティ部４０５に復号させ、それにより得られたコマンドに応じた処理を実行するため、保守員は、保守点検項目に応じたコマンドの入力操作を行うことによって、制御機器４００αの保守点検を行うことができる（Ｓ５１０）。

【００２９】

例えば、保守員が設定データ取得コマンドを入力した場合、保守装置２００の保守処理実行部２０５は、コマンド名を保守点検作業履歴として制御機器情報保持部２０１に格納するとともに、そのコマンドに含まれていた制御量名に対応するアドレスを制御機器情報の機器情報から読み出す。さらに、設定データ取得コマンドおよびアドレスをセキュリティ部２０４に暗号化させ、それにより得られた暗号化データを含む処理実行リクエストを、制御機器４００αに接続されたインタフェースから出力する。この処理実行リクエストを受け付けた制御機器４００αの入出力制御部４０４は、まず、そのリクエストに含まれている暗号化データをセキュリティ部４０５に復号させ、ついで、復号により得られたアドレスが示す暗号化データを、復号により得られたコマンドに応じて暗号化設定データ保持部４０２から読み出し、それを、保守装置２００に接続されているインタフェースから出力する。制御機器４００αから暗号化データを受け付けた保守装置２００では、セキュリティ部２０４が、その暗号化データを、制御機器情報の暗号鍵で復号し、その結果得られた目標値データを、保守処理実行部２０５が、保守装置２００のディスプレイに表示させる。これにより、保守員は、制御対象に属する制御量の目標値として現在設定されているデータをディスプレイ上で確認することができる。

【００３０】

また、保守員が設定データ変更コマンドを目標値データとともに保守装置２００に入力した場合、保守装置２００の保守処理実行部２０５は、コマンド名および目標値データを保守点検作業履歴として制御機器情報保持部２０１に格納するとともに、そのコマンドに含まれていた制御量名に対応するアドレスを制御機器情報の機器情報から読み出す。さらに、設定データ変更コマンド、目標値データおよびアドレスをそれぞれセキュリティ部２０４に暗号化させ、それにより得られた暗号化データを含む処理実行リクエストを、制御機器４００αに接続されたインタフェースから出力する。この処理実行リクエストを受け付けた制御機器４００αの入出力制御部４０４は、まず、処理実行リクエストに含まれている暗号化データのうち、設定データ変更コマンドの暗号化データおよびアドレスの暗号化データをセキュリティ部４０５に復号させ、ついで、復号により得られたアドレスが示す暗号化データを、復号により得られたコマンドに応じて、処理実行リクエストに含まれていた目標値データの暗号化データで更新し、その旨を制御処理実行部４０３に通知する。制御処理実行部４０３は、この通知を受け付けると、セキュリティ部４０５に、暗号化設定データ保持部４０２の暗号化データを機器ＩＤ／暗号鍵保持部４０１の暗号鍵で復号させ、それにより得られた目標値データとセンサ出力とを用いて、以後、制御対象の制御処理を実行する。

【００３１】

このようにして、保守員は、保守点検項目に応じたコマンドの入力操作を行うことによって制御機器４００αの保守点検を行い、その作業が終了したら、作業終了コマンドを保守装置２００に入力する必要がある（Ｓ５１１）。このコマンドを受け付けた保守装置２００の保守処理実行部２０５は、まず、制御機器情報保持部２０１から保守点検作業履歴を読み出して、その保守点検作業履歴と現在の日付と機器ＩＤとを含む登録リクエストの送信を保守内容送信部２０７に指示する。これにより、保守員による保守点検作業履歴と現

在の日付と機器ＩＤとを含む登録リクエストが保守管理ホスト１１２に送信される（Ｓ５１２）。保守管理ホスト１１２の保守履歴管理部１１３は、この登録リクエストに応じて、そのリクエストに含まれていた情報（機器ＩＤ、日付、保守点検作業履歴）を、新たな保守情報として保守情報データベース１２２に登録してから、データベース登録に成功した旨のメッセージを返信する（Ｓ５１３）。

【００３２】

このメッセージを受け付けたら、保守装置２００の保守処理実行部２０５は、さらに、制御機器情報保持部２０１からの全情報（制御機器情報、保守点検作業履歴）の削除を制御機器情報削除処理部２０４に実行させる（Ｓ５１４）。これにより、保守プログラムは終了する。最後に、図１６に示すように、保守員が保守装置２００の電源を切ると、ＲＡＭ上にロードされたデータも消去される。ここでは、保守プログラム終了前に制御機器情報保持部２０１から制御機器情報等が削除されるようにしているが、必ずしも、このようにする必要はない。例えば、保守装置の起動時に制御機器情報保持部２０１の全情報が削除されるようにしてもよいし、保守プログラム終了時または保守員認証実行時から、予め設定された時間が経過したら、制御機器情報保持部２０１の全情報が削除されるようにしてもよい。

【００３３】

本実施の形態に係る保守管理処理によれば、保守対象となる各制御機器の保守処理に必要な保守プログラム等を保守管理ホストに一元的に管理させ、保守員が、保守点検作業に必要な制御機器情報を保守管理ホストから保守装置にダウンロードすることができるようにしているため、保守員は、１台の保守装置を携帯しているだけで、様々な機種の制御機器の保守点検作業を行うことができる。そして、保守管理ホストには正規の保守員のみアクセスが許容されるため、保守管理ホストが管理している制御機器情報への不正アクセスを防止することができる。このため、制御機器の設置地点間を移動する保守員の便宜を図りつつ、制御機器に関する技術情報を不正アクセスから保護することができる。

【００３４】

また、保守点検作業が終了すれば、保守管理ホストからダウンロードされた制御機器情報が保守装置から消去されるため、保守員が携帯中の保守装置を紛失した場合等であっても、保守員が保守点検を完了した制御機器の機器情報の機密性が保たれる。このため、保守装置が盗難された場合等においても、制御機器に関する技術情報の安全性が確保される。

【００３５】

さらに、保守対象となる制御機器は、制御対象に属する制御量の目標値を暗号文で保持し、その暗号文の復号により得られたデータだけを制御対象の制御に用いるため、制御量の不正改ざんを防止することができる。このため、制御機器が制御対象とする装置の運行の安全性が確保される。

【００３６】

なお、ここでは、保守管理ホストからダウンロードされた制御機器情報がフラッシュメモリに格納されるようにしているため、制御機器情報を削除する処理を保守装置が実行するようにしているが、保守管理ホストからダウンロードされた制御機器情報がＲＡＭに保持されるだけの場合には、保守装置の電源ＯＦＦにより、ＲＡＭ上の制御機器情報が消去されるため、制御機器情報を削除する処理を保守装置が実行する必要はない。

【００３７】

つぎに、この制御機器保守管理システムの具体的な適用例について説明する。本実施の形態に係る制御機器保守管理システムは、例えば、各地に点在する制御機器の保守管理を請け負った保守会社、製造ライン上に複数の製造機器が点在する工場等に適用することができる。そこで、これら２つの適用例について説明する。

（１）保守会社への適用例

図８により、各地に点在する制御機器の保守管理を請け負った保守会社に、図１の制御機器保守管理システムを適用した場合について説明する。ここでは、昇降機制御機器を制御機器保守管理システムの保守対象とする場合を例に挙げる。

【００３８】
昇降機制御機器群４００の各機器には、それぞれ、制御対象の昇降機７１０が接続されている。各制御機器に搭載されたマイクロコンピュータが実現する制御処理実行部４０３は、昇降機７１０に搭載されたセンサの出力と暗号化データの復号により得られるデータ（目標値）とに基づいて、昇降機７１０の電気系統（モータ等）に与える制御指令を生成するようになっている。
【００３９】
このような昇降機制御機器群４００の保守管理を依頼された保守会社７００が図１の制御機器保守管理システムを採用した場合、管理システム１００は、保守会社７００内に設置される。
【００４０】
そして、管理システム１００の外部記憶装置１２０に格納される機器情報には、制御対象に属する制御量のうち、保守員による保守点検が許容された制御量の目標値として設定されたデータのアドレスが含まれる。例えば、各フロアにおけるドア開閉時間の調整が保守点検項目に含まれている場合には、外部記憶装置１２０の機器情報には、図９に示すような、各階のドア開閉時間パラメータの名前１２３Ａおよびアドレス１２３Ｂの対応情報１２３が含まれる。この対応情報を含む機器情報をダウンロードした保守装置２００は、制御量名「１階ドア開時間」を含む設定データ取得コマンドの入力を保守員から受け付けると、制御量名「１階ドア開時間」に対応付けられたアドレス「０×０２００」を含む設定データ送信リクエストを昇降機制御機器４００αに送信する。また、昇降機のモータ回転数の調整が保守点検項目に含まれている場合には、外部記憶装置１２０の機器情報には、モータ回転数パラメータの名前およびアドレスの対応情報を含めればよい。
【００４１】
そして、保守会社４００に所属する保守員は、昇降機制御機器群４００のうち、自己が担当する昇降機制御機器４００αの設置場所に赴き、その昇降機制御機器４００αに保守装置２００をシリアルケーブルで接続すれば、その昇降機制御機器４００αについて上述の保守管理処理を実行することができる。なお、保守装置２００と保守管理ホスト１１０とをつなぐネットワーク３００としては、インターネットを利用すればよい。
【００４２】
このように、図１の制御機器保守管理システムを昇降機制御機器の保守管理に適用した場合にも、もちろん、上述した効果と同様な効果が得られる。すなわち、正規の保守員のみアクセスが許可される保守管理ホストで制御機器情報が一元的に管理されているため、保守員は、１台の保守装置を携帯しているだけで、顧客ごとに異なる機種の昇降機制御機器の保守点検作業を行うことができる。そして、保守管理ホストには正規の保守員のみアクセスが許容されるため、保守管理ホストが管理している制御機器情報への不正アクセスを防止することができる。また、保守点検作業が終了した昇降機制御機器用の制御機器情報が保守装置に残らないため、昇降機制御機器に関する技術情報の安全性が確保される。さらに、昇降機制御機器に制御量の目標値を暗号文で保持させることによって、制御量の目標値の不正改ざん防止を図っているため、顧客の昇降機の運行安全性が確保される。
【００４３】
また、本実施の形態に係る制御機器保守管理システムを保守会社に適用すれば、保守会社の保守管理ホストで、各制御機器に対する保守点検作業履歴を管理することができるため、各制御機器に対する保守点検作業の内容に応じた料金の決済を、保守会社の保守管理ホストが銀行の決済システムに依頼することも可能となる。このようにする場合には、図１１に示すように、保守会社７００の保守管理ホストだけでなく、保守会社７００と保守契約７０３を結んだ顧客７０２の情報処理装置、保守会社７００および顧客７０３と取引契約を結んだ銀行７０１の決済システムがそれぞれインターネット３００に接続されている必要がある。さらに、保守装置２００には伝票印字装置を設けておく必要がある。そして、保守コマンド名と料金との対応付けた料金表データを管理システム１００の外部記憶装置１２０に格納しておき、保守管理ホスト１１２および保守装置２００が、図１２に示す

ように、前述のＳ５１３に代えて、以下の処理Ｓ５１３Ａを実行するようにする。

【００４４】

保守装置からの登録リクエストが保守管理ホスト１１２に送信されると（Ｓ５１２）、保守管理ホスト１１２の保守履歴管理部１１３は、新たな保守情報を保守情報データベース１２２に登録するとともに、その新たな保守情報の保守点検作業履歴に含まれていた各コマンド名に対応付けられた料金を料金表データから読み出し、それらの料金の合計金額を、顧客７０２に対する請求金額として算出する。そして、この請求金額とともに、データベース登録に成功した旨のメッセージを返信する（Ｓ５１３Ａ）。

【００４５】

このメッセージ等を受け付けたら、保守装置２００の保守処理実行部２０５は、図１０に示すような保守点検内容表示画面２１０をディスプレイに表示させる（Ｓ５１３Ｂ）。この保守点検内容表示画面２１０には、保守点検作業履歴に含まれているコマンド名のリスト２１１、顧客に対する請求金額２１２、保守点検内容表示画面２１０上の表示情報の印字指示を受け付けるＯＫボタン２１３、保守点検内容表示画面２１０の消去指示を受け付けるキャンセルボタン２１４が表示されている。この画面上のＯＫボタン２１３に保守員がタッチすると、保守管理ホスト１１２の保守履歴管理部１１３が、伝票印字装置に保守点検内容表示画面２１０上の表示情報を印字させる。保守員は、この伝票を顧客７０２に提示することよって、保守現場で、料金についての承認を顧客から得ることができる。

【００４６】

そして、保守点検内容表示画面２１０上の表示情報の印字が終了したら、保守装置２００の保守処理実行部２０５は、Ｓ５１４の削除処理を制御機器情報削除処理部２０４に実行させる。

【００４７】

一方において、保守管理ホスト１１２の保守履歴管理部１１３は、顧客７０２に対する請求金額、顧客７０２の識別情報および保守会社７００の識別情報を含む決済リクエストを、適当なタイミングで、銀行７０１の決済システムに送信する（Ｓ５１６）。銀行７０１の決済システムは、そのリクエストに含まれる情報に基づき、保守会社７００および顧客７２に対する決済処理をオンラインで実行する（Ｓ５１７）。

【００４８】

このような処理によれば、保守会社は、制御機器ごとに、その制御機器について作業員が行った保守点検の内容を保守履歴として管理しているため、制御機器の保有者（顧客）に対して、保守点検の内容に応じた課金をすることができる。

（２）工場への適用例

図１３により、製造ライン上に複数の製造機器が点在する工場に、図１の制御機器保守管理システムを適用した場合について説明する。ここでは、製造装置の制御機器を、制御機器保守管理システムの保守管理対象とする場合を例に挙げる。

【００４９】

各製造装置の制御機器に搭載されたマイクロコンピュータが実現する制御処理実行部４０３は、製造ライン３０１に設置されたセンサの出力と暗号化データの復号により得られるデータ（目標値）とに基づいて、製造装置の電気系統（モータ等）に与える制御指令を生成するようになっている。

【００５０】

このような制御機器群４００が設置された工場８００が図１の制御機器保守管理システムを採用した場合、管理システム１００は、工場内のいずれかの箇所に設置される。

【００５１】

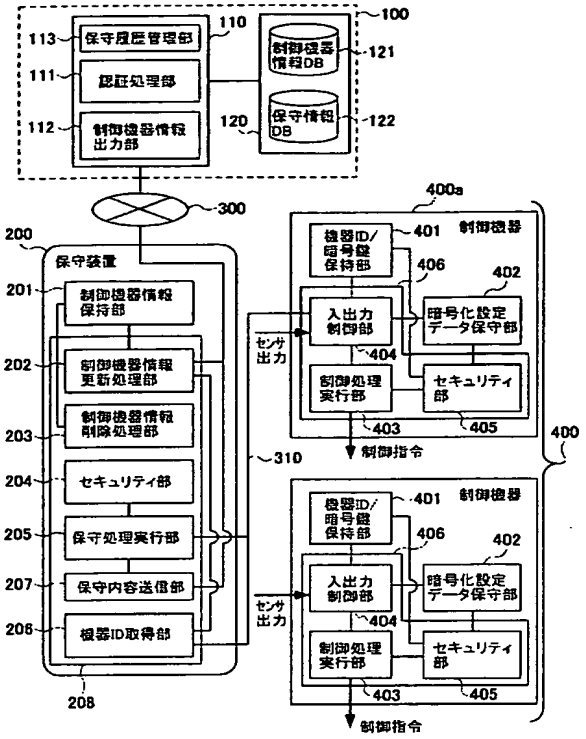
そして、管理システム１００の外部記憶装置１２０に格納される機器情報には、制御機器の制御対象に属する制御量のうち、保守員による保守点検が許容された制御量の目標値として設定された目標値のアドレスが含まれる。例えば、製造装置８０２のモータ回転数の調整が保守点検項目に含まれている場合には、外部記憶装置１２０の機器情報には、モータ回転数パラメータの名前およびアドレスの対応情報を含まれる。

【００５２】
そして、保守員は、保守装置２００を携帯しながら工場８００内を巡回し、各制御機器に保守装置２００をシリアルケーブルで接続することによって、工場８００内の各制御機器について上述の保守管理処理を実行することができる。なお、保守装置２００と保守管理ホスト１１０とをつなぐネットワーク３００は、工場８００内に配置された無線基地局で構成すればよい。
【００５３】
このように、図１の制御機器保守管理システムを工場８００内の製造装置８０２の制御機器の保守管理に適用した場合にも、もちろん、上述した効果と同様な効果が得られる。すなわち、正規の保守員のみアクセスが許可される保守管理ホストで制御機器情報が一元的に管理されているため、保守員は、１台の保守装置を携帯しているだけで、工場内に点在する様々な機種の製造装置の制御機器の保守点検作業を行うことができる。そして、保守管理ホストには正規の保守員のみアクセスが許容されるため、保守管理ホストが管理している制御機器情報への不正アクセスを防止することができる。また、保守点検作業が終了した制御機器用の制御機器情報が保守装置に残らないため、工場内の製造機器に関する技術情報の安全性が確保される。さらに、制御量の目標値の不正改ざんが防止されるため、製造ラインの運行の安全性が確保される。
【００５４】
なお、以上においては、保守員が暗記しているパスワードおよびユーザＩＤを認証情報に基づきユーザ認証が行われしているが、保守員の持ち物または身体的特徴を利用したユーザ認証が行われるようにしてもよい。
【００５５】
例えば、カードスロットが保守装置２００に設けられている場合、または、図１４に示すように、カードリーダ２１０が保守装置２００に接続されている場合には、各保守員に認証情報を暗記させる代わりに、保守員の認証情報（ユーザＩＤ等）を記憶させたＩＤカード（ＩＣカード等）２１１を各保守員に携帯させておくようにしてもよい。この場合には、保守装置２００の制御機器情報更新処理部２０２が、ユーザ認証画面の代わりに、カードスロットまたはカードリーダ２１０へのＩＤカード装着を促すメッセージをディスプレイに表示させ、その後、カードスロットまたはカードリーダ２１０へのＩＤカード装着を検知すると、そのＩＤカード２１１から認証情報を読み取って、それを保守管理ホストに送信するようにすればよい。
【００５６】
または、指紋の特徴点を抽出する指紋認識装置が保守装置２００に接続されている場合には、保守員の指紋の特徴点を、保守員の認証情報として用いるようにしてもよい。この場合には、保守装置２００の制御機器情報更新処理部２０２が、ユーザ認証画面の代わりに、指紋識別装置への指接触を促すメッセージをディスプレイに表示させ、指紋識別装置からの出力を保守管理ホストに送信するようにすればよい。
【００５７】
このように、保守員の持ち物または身体的特徴を利用したユーザ認証を行うようにすれば、保守員は、
保守装置の認証のために特段の手段を用意することなく既に保持しているＩＤカードを用いることができ、導入時の工数を削減できる。
【００５８】
【発明の効果】
本発明によれば、保守対象機器に関する技術情報のセキュリティを向上させることができる。
【図面の簡単な説明】
【図１】本発明の実施の一形態に係る制御機器保守システムの全体構成図である。
【図２】制御機器情報データベースのデータ構造を概念的に示した図である。
【図３】保守情報データベースのデータ構造を概念的に示した図である。

【図４】パスワードファイルに記述された情報を概念的に示した図である。
【図５】保守スケジュールファイルに記述された情報を概念的に示した図である。
【図６】図１の制御機器保守システムで実行される保守管理処理の流れを示すチャート図である。
【図７】ユーザ認証画面上のレイアウト例を示した図である。
【図８】昇降機制御機器の保守管理を請け負った保守会社に適用された場合の、本発明の実施の一形態に係る制御機器保守システムの全体構成図である。
【図９】図８の管理ホストが管理している機器情報のデータ構造を概念的に示した図である。
【図１０】認証保守点検内容表示画面上のレイアウト例を示した図である。
【図１１】保守会社、銀行および顧客の間の契約関係を説明するための図である。
【図１２】図１１の制御機器保守システムで実行される保守管理処理の流れを示すチャート図である。
【図１３】複数の製造装置の制御機器が点在する工場に適用された場合の、本発明の実施の一形態に係る制御機器保守システムの全体構成図である。
【図１４】本発明の実施の一形態に係る保守装置と、保守員の認証情報の入力に利用されるカードリーダとの接続図である。
【図１５】複数の制御機器のうちの１台の保守点検作業中の保守装置の状態を示した図である。
【図１６】保守装置の電源断状態を示した図である。
【符号の説明】
１００　管理システム、１１０　情報処理装置（保守管理ホスト）、
１１１　認証処理部、１１２　制御機器情報出力部、
１１８　保守履歴管理部、１２０　外部記憶装置、
１２１　制御機器情報データベース、１２２　保守情報データベース、
２００　携帯情報端末（保守装置）、２０１　制御機器情報保持部、
２０２　制御機器情報更新処理部、２０３　制御機器情報削除処理部、
２０４　セキュリティ部、２０５　保守処理実行部、
２０６　機器ＩＤ取得部、２０７　保守内容送信部、２０８　制御部
４００　制御機器群、４０１　機器ＩＤ／暗号鍵保持部、
４０２　暗号化設定データ保持部４０３　演算処理部、
４０４　入出力制御部、４０５　セキュリティ部、
４０６　制御処理実行部

【図１】

図1



【図２】

図2

121A ID	121B 保守プログラム	機器情報	121C 暗号鍵
A20005589	addr1-1	addr2-1	0xA001060701FEB03120
A20005590	addr1-2	addr2-2	B03120FEA001060701 0x

【図３】

図3

122A ID	122B 保守日付	122C 作業内容
A20005589	2002.10.1	設定データ変更情報・・・
A20005590	2002.10.1	設定データ変更情報・・・

【図４】

図4

114	
114A ユーザID	114B パスワード
USR1	*****
USR2	****
USR3	*****

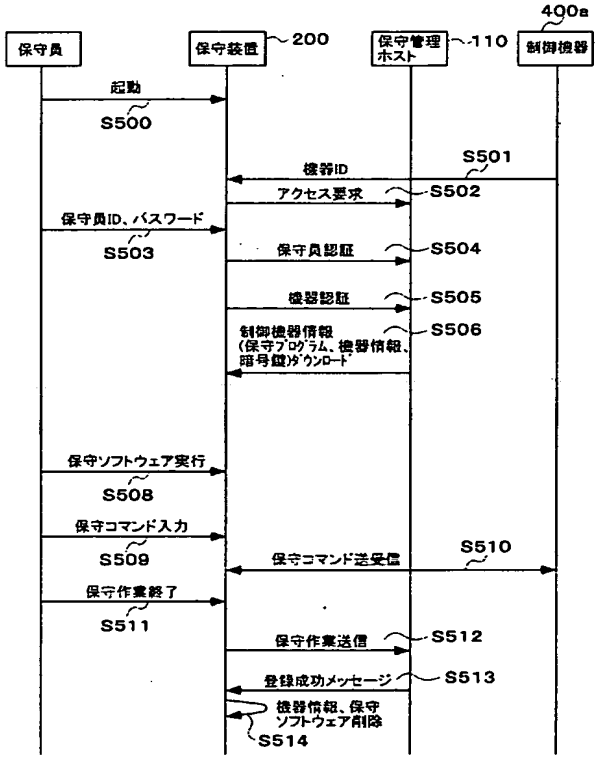
【図５】

図5

115	115				
ユーザID	1		2		
	機器ID	日付	機器ID	日付	
USR1	A20005589	2002.10.1	A20005590	2002.10.1	
USR2	A20005591	2002.10.2	A20005592	2002.10.3	

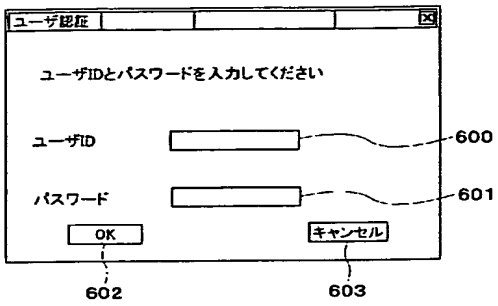
【図６】

図6



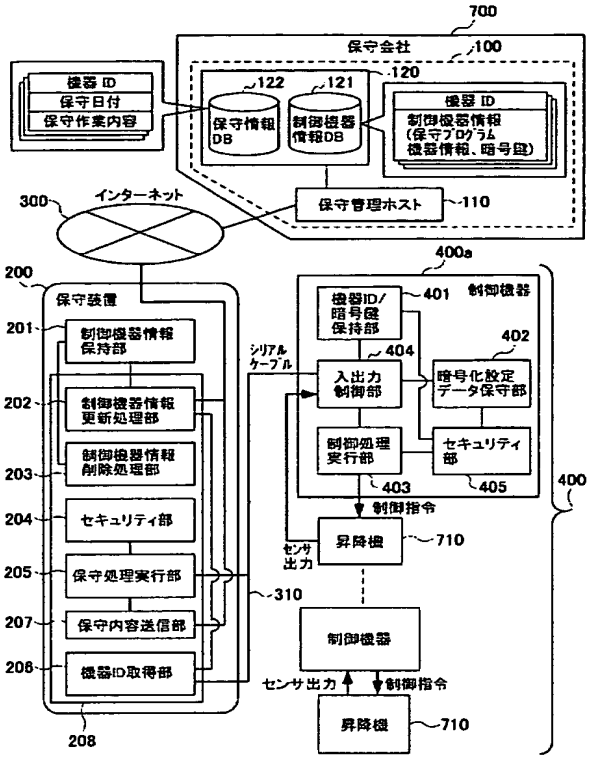
【図７】

図7



【図８】

図8



【図９】

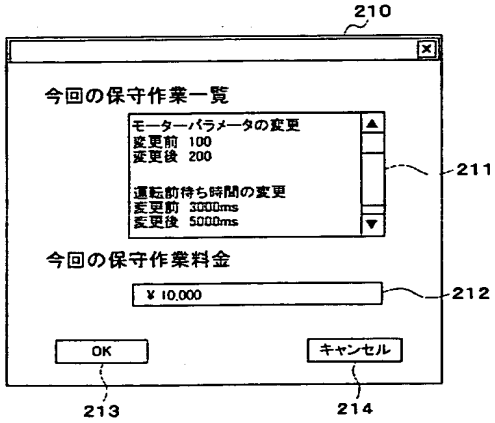
図9

123

123A 名称	123B アドレス
1階ドア開時間	0x0200
2階ドア開時間	0x0204
3階ドア開時間	0x0208
:	:

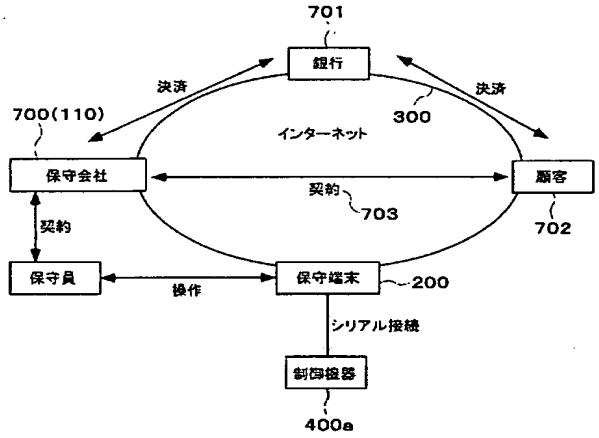
【図１０】

図10



【図１１】

図11



【図１２】

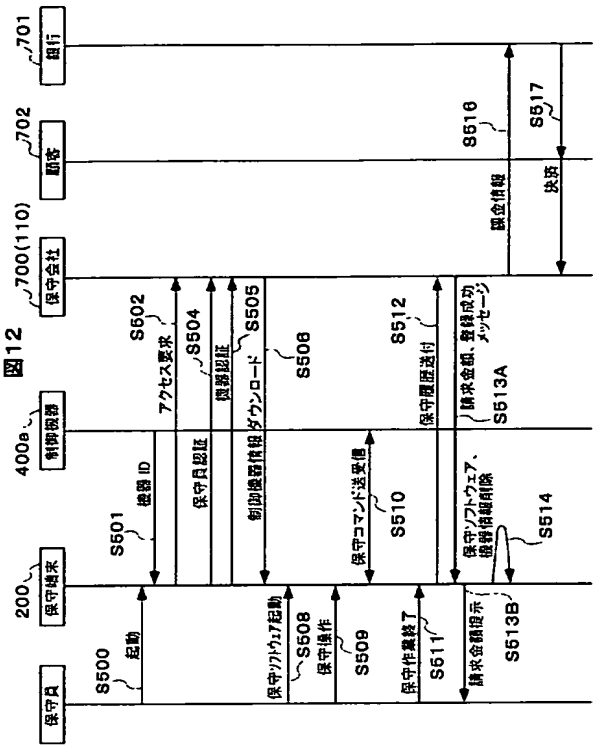
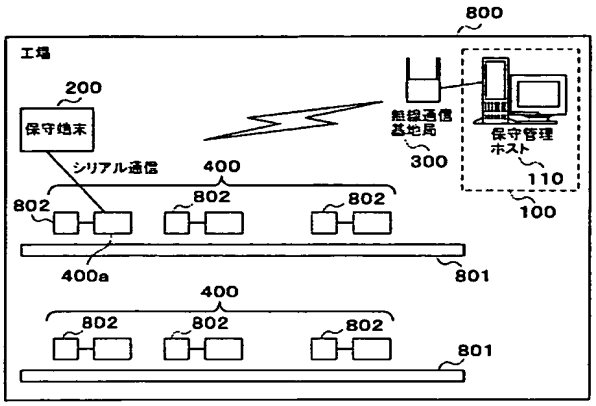


図12

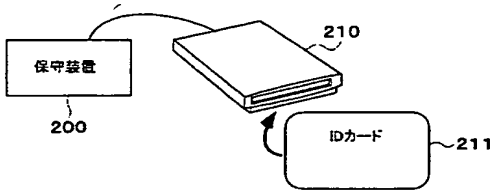
【図１３】

図13



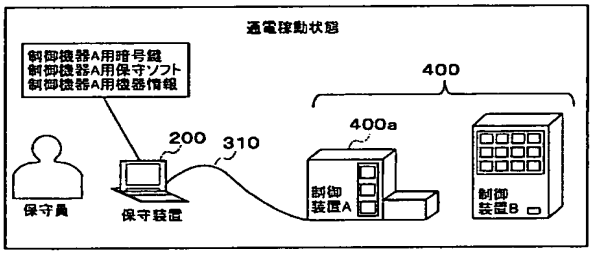
【図１４】

図14



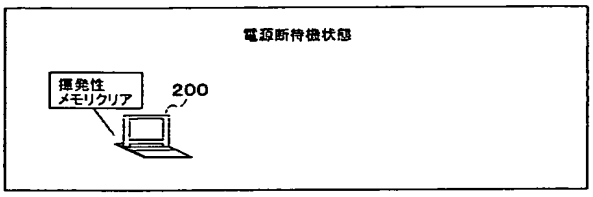
【図１５】

図15



【図１６】

図16



フロントページの続き

(51)Int.Cl.[7]	FI			テーマコード（参考）
	H04Q	9/00	321D	
	H04Q	9/00	341Z	
	H04L	9/00	601A	
	H04L	9/00	673E	

Fターム(参考) 5J104 AA12 AA16 EA04 EA08 MA01 NA02
5K048 AA15 BA51 EB12 HA02